HTTPS

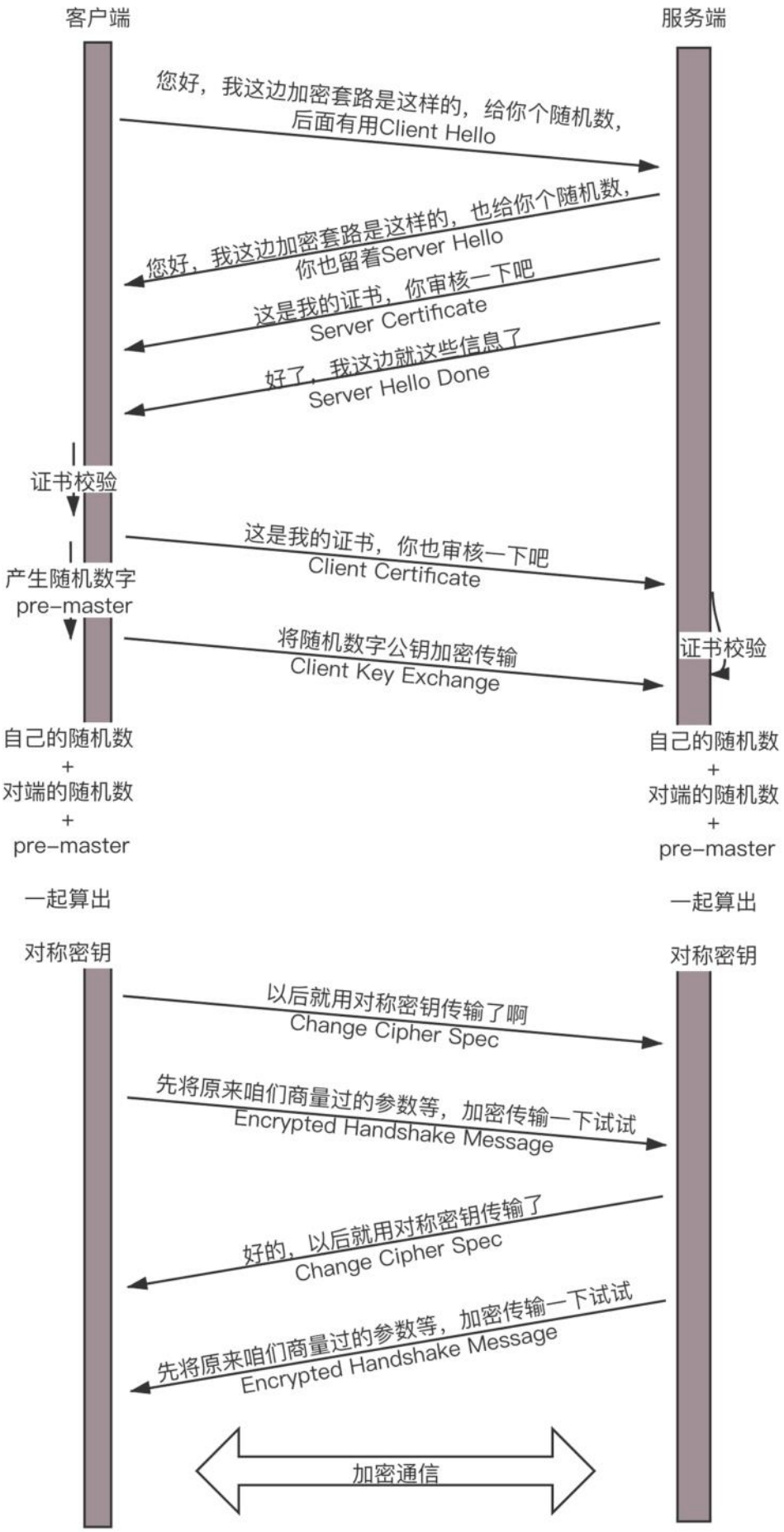
2022年4月27日 16:01

加密

1. 对称
    a. 相同的key 加密解密
2. 非对称
    a. Public key加密，private key解密
3. 怎么确定你给我的pullic key 真的是你的
    a. 证书解密签名的方式
4. X.509编码格式
    a. PEM
    打开看文本格式，以“-----BEGIN…”开头，“-----END…”结尾，内容是 BASE64 编码。
    Apache 和 UNIX 服务器偏向于使用这种编码格式。
    b. DER
    打开看是二进制格式，不可读。
    Java 和 Windows 服务器偏向于使用这种编码格式。
5. 相关的文件扩展名
    1、CRT
    CRT 应该是 certificate 的三个字母，其实还是证书的意思。常见于 UNIX 系统，有可能是 PEM 编码，也有可能是 DER 编码，大多数应该是 PEM 编码，相信你已经知道怎么辨别。
    2、CER
    还是 certificate，还是证书。常见于 Windows 系统，同样的可能是 PEM 编码，也可能是 DER 编码，大多数应该是 DER 编码。
    3、KEY
    通常用来存放一个公钥或者私钥，并非 X.509 证书。编码同样的，可能是 PEM，也可能是 DER。
    4、CSR
    Certificate，Signing Request，即证书签名请求。这个并不是证书，而是向权威证书颁发机构获得签名证书的申请，其核心内容是一个公钥（当然还附带了一些别的信息）。在生成这个申请的时候，同时也会生成一个私钥，私钥要自己保管好。做过 iOS APP 的朋友都应该知道是，怎么向苹果申请开发者证书的吧。

HTTPS 的工作模式

公钥私钥主要用于传输对称加密的秘钥，而真正的双方大数据量的通信都是通过对称加密进行的。


客户端
服务端
您好，我这边加密套路是这样的，给你个随机数，
后面有用Client Hello
您好，我这边加密套路是这样的，也给你个随机数，
你也留着Server Hello
这是我的证书，你审核一下吧
Server Certificate
好了，我这边就这些信息了
Server Hello Done
证书校验
这是我的证书，你也审核一下吧
Client Certificate
产生随机数字
pre-master
将随机数字公钥加密传输
Client Key Exchange
证书校验
自己的随机数
+
对端的随机数
+
pre-master
一起算出
对称密钥
自己的随机数
+
对端的随机数
+
pre-master
一起算出
对称密钥
以后就用对称密钥传输了啊
Change Cipher Spec
先将原来咱们商量过的参数等，加密传输一下试试
Encrypted Handshake Message
好的，以后就用对称密钥传输了
Change Cipher Spec
先将原来咱们商量过的参数等，加密传输一下试试
Encrypted Handshake Message
加密通信